Section C - Description/Specifications/Statement of Work

1.0 SCOPE

The contractor shall support the Naval Surface Warfare Center, Port Hueneme Division (NSWC PHD) Information Technology (IT) team to develop formal plans and set realistic milestones, objectives and deadlines. The contractor shall support the requirements of a complex matrix organization, supporting various sponsor driven requirements with the goal of developing IT tools that can be leveraged across organizational boundaries. In addition to operating and maintaining the current Navy standard / Research, Development, Test and Evaluation (RDT&E) applications and infrastructure, NSWC PHD requires continuous visibility into emerging technologies, seeking more efficient and effective ways of accomplishing both mission and business tasking. A systems approach to an integrated IT architecture infrastructure, operating in a Navy-accredited Network environment is the driving imperative in all applications and considerations. The scope of the effort also includes sustaining compliance with applicable Department of the Navy (DoN) Cybersecurity Policy.

2.0 APPLICABLE DOCUMENTS

The contractor shall comply with all documents listed below as mandatory and support all efforts under paragraph 3.0 of this SOW. All of the documents listed herein are assumed to be the latest revision as of the date of award. The most current version of all documents applies through the life of this task order.

TITLE	DESCRIPTION	LINK
10 U.S.C. 2222	Defense Business Systems: Architecture, Accountability, and Modernization	http://uscode.house.gov/view.xhtml?req=(title:10%20section:2222%20edition:prelim
DODDIR 8000.1	Management of the DoD Information Enterprise	www.dtic.mil/dtic/tr/fulltext/u2/a256988.pdf
DODINST 8500.01	Cybersecurity	https://fas.org/irp/doddir/dod/i8500_01.pdf
DODINST 8510.01	RMF for DoD IT	http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf

DODINST 8140	Cyberspace Workforce Improvement Program	https://www.sans.org/dodd-8140/
CJCSI 6510.01F	IA and Support to Computer Network Defense	http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf
SECNAVINST 5000.36A	DoN IT Applications and Data Management	http://www.doncio.navy.mil/contentview.aspx?id=348
SECNAV M-5510.36	DoN Information Security Program (ISP) Instruction	http://www.secnav.navy.mil/dusnp/Security/Information/Documents/SECNAVINST%205510.36A.pdf
SECNAVINST M-5239.2	DoN IA Workforce Management Manual to Support the Cybersecurity Workforce Improvement Program	https://fas.org/irp/doddir/navy/secnavinst/5239_3c.pdf
SECNAVINST 5239.3B	DoN IA Policy	http://www.doncio.navy.mil/uploads/0629gtm45215.pdf
OPNAVINST 5239.1C	Navy IA Program	http://doni.daps.dla.mil/Directives/05000%20General%20Management%20Security%20and%20Safety%20Services/05-200%20Management%20Program%20and%20Techniques%20Services/5239.1C.pdf
NAVSEAINST 5239.2A	Naval Sea Systems Command (NAVSEA) Cybersecurity IA Program	https://www.cool.navy.mil/usn/ia_documents/5239_NCF_Cybersecurity_IA_HANDBOOK.pdf
NIST SP 800-53	Security and Privacy Controls for Federal Information Systems and Organizations	https://nvd.nist.gov/800-53

DODINST 5025.1-M	DoD Directives Program	https://fas.org/irp/doddir/dod/d5025_01.htm
ISO/IEC 20000	Standard for IT service management	http://www.iso.org/iso/catalogue_detail?csnumber=51986
IEEE/EIA 12207	Standard for Information Technology - Software Life Cycle Processes	http://standards.ieee.org/findstds/standard/12207.0-1996.html
	Federal Information Processing Standards Publications	http://www.nist.gov/itl/fips.cfm
	DISA STIGs	

3.0 REQUIREMENTS

3.1 GENERAL REQUIREMENTS

3.1.1 Non-Personal Services

If the contractor perceives any actions to constitute personal services, the contractor shall notify the Contracting Officer immediately.

3.1.2 Business Relations

The contractor shall provide corrective action plans, proposal submittals, timely identification of issues, and effective management of subcontractors. The contractor shall seek to ensure customer satisfaction and professional and ethical behavior of all contractor personnel.

3.1.3 Contractor Program Management

The contractor shall establish clear organizational lines of authority and responsibility to ensure effective management of the resources assigned to the requirement and shall maintain continuity of operations at all times.

The contractor shall respond to Government requests for contractual actions in a timely fashion. The contractor shall maintain a single point of contact for management of all efforts.

The contractor shall provide the management and support required to adequately perform the tasking of this requirement. The contractor shall ensure their employees' capabilities and skills remain current by providing initial and refresher training as required to meet the SOW requirements. The contractor shall provide necessary infrastructure to support contract tasks.

The contractor shall accomplish the assigned work by employing and utilizing qualified personnel with appropriate combinations of education, training, and experience. The contractor team must adhere to paragraph 2.0 (Applicable Directives) of this SOW. All contractor resources must be able to work independently and maintain a mastery skill set of the technologies supported, both for systems as currently implemented and as technologies are introduced for implementation.

Key Position 1: Senior Systems Engineer (Windows, Linux, VMWare, Host Based Security System (HBSS), Storage Area Network (SAN))

a) REQUIRED QUALIFICATIONS:

- Minimum of 10 years of Windows and 5 years of Linux server technologies experience including Active Directory, Group Policy Management and Public Key Infrastructure (PKI) implementation
- Minimum of five years of VMWare Infrastructure experience
- Minimum of five years of SAN/Blade Server infrastructure experience
- Minimum of five years of experience in Information Security requirement implementations including the ability to ensure Information Assurance (IA) Vulnerability Alert (IAVA)/M and Defense Information Systems Agency (DISA) Security Technical Implementation Guidelines (STIG) compliance
- Minimum of five years of experience with HBSS implementations including the configuration and monitoring of HBSS Fragmentary Orders
- Minimum of five years of experience with Department of Defense (DoD) Cybersecurity controls including the use of STIGs, SRRs, and Assured Compliance Assessment Solution (ACAS) implementation

b) DESIRED QUALIFICATIONS:

- Experience with fibre channel fabric/zoning/logical unit number management
- HP 3PAR and cClass Blade architecture experience, or equivalent platform capabilities
- Experience with disaster recovery preparedness and administration using policy based backup applications

Key Position 2: Senior Systems Administrator (Cisco Routers, Switches, Intrusion Detection System (IDS)/Intrusion Prevention System (IPS), Firewall)

a) REQUIRED QUALIFICATIONS:

- Minimum of five years of Cisco layer 2 and layer 3 Infrastructure experience
- Minimum of five years of Firewall, IDS and/or IPS administration and configuration experience
- Experience with cabling management
- Minimum of five years securing a Cisco environment in accordance with DISA STIGs

b) DESIRED QUALIFICATIONS:

- Minimum of five years of experience with scoping, architecture and design of new network infrastructure including cryptographic and long haul requirements

Key Position 3: Senior Web Programmer

a) REQUIRED QUALIFICATIONS:

- Minimum of five years of experience related to the development of web-based applications using C#, .NET and Java technologies with emphasis in .NET application development.
- Minimum of five years securing a web environment in accordance with DISA STIGs.
- Experience directly related to the development of MS SQL driven applications.
- Experience in SharePoint 2016 and the ability to design and engineer SharePoint based enterprise solutions.
- Ability to develop Asynchronous JavaScript and Extensible Markup Language (XML) (AJAX) enabled .NET web Applications using Version Control Systems,
- Hypertext Transfer Protocol (HTTP) and the Representational State Transfer (ReST) architecture.
- Demonstrated expertise in configuration and administration of Microsoft Internet Information Services (IIS) and the .NET Framework, Integrated Windows Authentication, Kerberos and Directory Services Authentication, PKI, Secure Sockets Layer (SSL), troubleshooting, configuration and development.
- Minimum of five years of experience delivering, analyzing, and troubleshooting complex distributed systems.
- Demonstrated expertise in the implementation, integration, testing of enterprise application/database/web platforms.

b) DESIRED QUALIFICATIONS:

- Experience in using identity management and PKI infrastructure.
- Ability to develop C# .NET application(s) that interface with Active Directory Services.
- Experience with SOA development and implementations.
- Strong understanding of various programming languages, frameworks and technologies to include: ASP.NET (C#, Model-View-Controller (MVC), WCF, Data Services, Entity Framework, Language Integrated Query (LINQ) to SQL), PowerShell, AJAX, jQuery, JavaScript Object Notation (JSON), Java, SQL/Transact-SQL/Computer Language Research, XML, HTML, CSS, ReST.
- Experience with Microsoft PowerBI Stack.

Key Position 4: Senior Database Engineer

a) REQUIRED QUALIFICATIONS:

- Minimum of five years in the development and deployment of distributed relational databases and associated BI systems.
- Minimum of five years of experience with the Microsoft SQL server stack, Microsoft SQL, SQL Server Integration Services (SSIS), SQL Server Analysis Services (SSAS), and Microsoft SQL Server Reporting Services SSRS.
- Minimum of five years securing a SQL environment in accordance with DISA STIGs.
- Minimum of five years SQL Server configuration management, optimization, administration, development in client/server architecture, business object modeling and relational database design using MS SQL Server.
- Minimum of five years writing complex Transact SQL queries, stored-procedures and designing relational databases.

b) DESIRED QUALIFICATIONS:

- Experience with IBM Cognos and other On-Line Analytical Processing (OLAP) tools.
- Understanding of Navy Working Capital Fund (WCF) accounting principles and generation of reports / OLAP analysis from WCF funding and cost information.
- Experience leading and designing Service Oriented Architecture (SOA) based application.
- Experience in Navy Security requirements implementation and their impacts to overall software architecture.
- Experience with Microsoft PowerBI Stack.

Key Position 5: Senior Systems Security Engineer (eMASS, Risk Management Framework (RMF), ACAS, Vulnerability Remediation Asset Manager (VRAM), audit, monitor etc.)

a) REQUIRED QUALIFICATIONS:

- Minimum five years of experience with the DoD Cybersecurity Authorization & Accreditation processes and tools (to include RMF and eMASS)
- Minimum five years of Cybersecurity system auditing and monitoring experience (to include Inspector General inspection and Command Cyber Readiness Inspection criteria)
- Experience with the Navy's ACAS system and Navy's VRAM

b) DESIRED QUALIFICATIONS:

- Experience with DoD or DoN cybersecurity policies and procedures
- Experience managing DoD Cybersecurity Program requirements and deliverables
- Knowledge of HBSS, Firewall, IDS, and IPS

3.1.4 Travel

Travel to Government facilities other than NSWC PHD Port Hueneme or other contractor facilities may be required. Travel requirements will be specified via Technical Instruction.

3.1.5 Government Furnished Property

The Government will provide office space and communications capability for use by contractor personnel who are stationed onsite in the performance of this contract.

3.1.6 Safeguarding Covered Defense Information and Cyber Incident Reporting

3.1.6.1 System Security Plan and Plans of Action and Milestones (SSP/POAM) Reviews

a) Within 30 days of task order award, the contractor shall make its SSP(s) for its covered contractor information system(s) available for review by the Government at the contractor's facility. The SSP(s) shall implement the security requirements in Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, which is included in this task order. The contractor shall fully cooperate in the Government's review of the SSPs at the contractor's facility.

b) If the Government determines that the SSP(s) does not adequately implement the requirements of DFARS clause 252.204-7012 then the Government shall notify the contractor of each identified deficiency. The contractor shall correct any identified deficiencies within 30 days of notification by the Government. The contracting officer may provide for a correction period longer than 30 days and, in such a case, may require the contractor to submit a POAM for the correction of the identified deficiencies. The contractor shall immediately notify the contracting officer of any failure or anticipated failure to meet a milestone in such a POAM.

c) Upon the conclusion of the correction period, the Government may conduct a follow-on review of the SSP(s) at the contractor's facilities. The Government may continue to conduct follow-on reviews until the Government determines that the contractor has corrected all identified deficiencies in the SSP(s).

d) The Government may, in its sole discretion, conduct subsequent reviews at the contractor's site to verify the information in the SSP(s). The Government will conduct such reviews at least every three years (measured from the date of task order award) and may conduct such reviews at any time upon 30 days' notice to the contractor.

3.1.6.2 Compliance to NIST 800-171

a) The contractor shall fully implement the CUI Security Requirements (Requirements) and associated Relevant Security Controls (Controls) in NIST Special Publication 800-171 (Rev. 1) (NIST SP 800-171), or establish a SSP(s) and POAMs that varies from NIST 800-171 only in accordance with DFARS clause 252.204-7012(b)(2), for all covered contractor information systems affecting this task order.

b) Notwithstanding the allowance for such variation, the contractor shall identify in any SSP and POAM their plans to implement the following, at a minimum:

(1) Implement Control 3.5.3 (Multi-factor authentication). This means that multi-factor authentication is required for all users, privileged and unprivileged accounts that log into a network. In other words, any system that is not standalone should be required to utilize acceptable multi-factor authentication. For legacy systems and systems that cannot support this requirement, such as CNC equipment, etc., a combination of physical and logical protections acceptable to the Government may be substituted;

(2) Implement Control 3.1.5 (least privilege) and associated Controls, and identify practices that the contractor implements to restrict the unnecessary sharing with, or flow of, covered defense information to its subcontractors, suppliers, or vendors based on need-to-know principles;

(3) Implement Control 3.1.12 (monitoring and control remote access sessions) - Require monitoring and controlling of remote access sessions and include mechanisms to audit the sessions and methods.

(4) Audit user privileges on at least an annual basis;

(5) Implement:

i. Control 3.13.11 (FIPS 140-2 validated cryptology or implementation of NSA or NIST approved algorithms (i.e. FIPS 140-2 Annex A: AES or Triple DES) or compensating controls as documented in a SSP and POAM); and,

ii. NIST Cryptographic Algorithm Validation Program (CAVP) (see https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program);

(6) Implement Control 3.13.16 (Protect the confidentiality of CUI at rest) or provide a POAM for implementation which shall be evaluated by the Navy for risk acceptance.

(7) Implement Control 3.1.19 (encrypt CUI on mobile devices) or provide a plan of action for implementation which can be evaluated by the Government Program Manager for risk to the program.

3.1.6.3 Cyber Incident Response:

a) The contractor shall, within 15 days of discovering the cyber incident (inclusive of the 72-hour reporting period), deliver all data used in performance of the task order that the contractor determines is impacted by the incident and begin assessment of potential warfighter/program impact.

b) Incident data shall be delivered in accordance with the Department of Defense Cyber Crimes Center (DC3) Instructions for Submitting Media available at http://www.acq.osd.mil/dpap/dars/pgi/docs/Instructions_for_Submitting_Media.docx. In delivery of the incident data, the contractor shall, to the extent practical, remove contractor-owned information from Government covered defense information.

c) If the contractor subsequently identifies any such data not previously delivered to DC3, then the contractor shall immediately notify the contracting officer in writing and shall deliver the incident data within 10 days of identification. In such a case, the contractor may request a delivery date later than 10 days after identification. The contracting officer will approve or disapprove the request after coordination with DC3.

3.1.6.4 Naval Criminal Investigative Service (NCIS) Outreach

The contractor shall engage with NCIS industry outreach efforts and consider recommendations for hardening of covered contractor information systems affecting DON programs and technologies.

3.1.6.5 NCIS/Industry Monitoring

a) In the event of a cyber incident or at any time the Government has indication of a vulnerability or potential vulnerability, the Contractor shall cooperate with the NCIS, which may include cooperation related to: threat indicators; pre-determined incident information derived from the contractor's infrastructure systems; and the continuous provision of all contractor, subcontractor or vendor logs that show network activity, including any additional logs the contractor, subcontractor or vendor agrees to initiate as a result of the cyber incident or notice of actual or potential vulnerability.

b) If the Government determines that the collection of all logs does not adequately protect its interests, the contractor and NCIS will work together to implement additional measures, which may include allowing the installation of an appropriate network device that is owned and maintained by NCIS, on the contractor's information systems or information technology assets. The specific details (e.g., type of device, type of data gathered, monitoring period) regarding the installation of an NCIS network device shall be the subject of a separate agreement negotiated between NCIS and the contractor. In the alternative, the contractor may install network sensor capabilities or a network monitoring service, either of which must be reviewed for acceptability by NCIS. Use of this alternative approach shall also be the subject of a separate agreement negotiated between NCIS and the contractor.

c) In all cases, the collection or provision of data and any activities associated with this statement of work shall be in accordance with federal, state, and non-US law.

3.1.7 Transition

The contractor shall follow the transition plan submitted as part of their proposal and keep the Government fully informed of status throughout the transition period. Throughout the phase-in/phase-out periods, it is essential that attention be given to minimize interruptions or delays to work in progress that would impact the mission. The contractor must plan for the transfer of work control, delineating the method for processing and assigning tasks during the phase-in/phase-out periods (CDRL A006).

3.2 PERFORMANCE REQUIREMENTS

The following paragraph specifies the Performance Objectives and Performance Elements for the contract.

3.2.1 Operations and Maintenance

Contractor shall provide IT professionals who have an expert knowledge and experience in the oversight of corporate computing plants.

3.2.1.1 Operations and Systems Support

The contractor shall provide continuous support for the command's computing plant that supports the NSWC PHD Command Corporate and RDT&E infrastructures (both unclassified and classified up to and including Secret), and Secure Internet Protocol Network (SIPRNET) which are critical to accomplish NSWC PHD's mission. Support services will include server, network, application, and database administration as well as OS upgrades and security patches required to maintain operational availability and full compliance with current Cybersecurity requirements. Server, cloud and application support is required 24 hours a day, seven days a week for the entire performance of this contract.

The contractor shall provide technical support to customers for in-scope systems/applications.

The contractor shall provide primary and back-up personnel in support of functions related hardwiring, installing and upgrading phone and data cable plant.

The contractor shall provide support services to include communicating with internal and external parties who request

VTC support, scheduling VTC bridges in support of pre-defined meeting requirements and set-up and/or tear-down of scheduled VTC conferences.

The contractor shall perform installation, configuration, operation and advanced troubleshooting of standards-based video conference hardware, software and ancillary media center equipment.

The contractor shall have an advanced understanding of H.323/SIP VTC transport and session protocols, firewall traversal software/hardware and conference bridging applications.

The contractor shall ensure equipment is properly maintained and ready to support scheduled command conference room events on an on-going and ad-hoc basis.

The contractor shall perform technical operation, as well as troubleshooting, of all media center hardware, including displays, microphones, amplifiers, video switchers and system controllers.

The contractor shall provide technical assistance with video network infrastructure design, system topology and application of DoD IA policies for securing an IP-based VTC environment in accordance with STIG.

The contractor shall ensure equipment is properly maintained and ready to support scheduled command conference room events on an on-going basis.

The contractor shall make hardware upgrades and system modifications to all systems which are not covered by the Navy Services contract (e.g. NMCI).

The contractor shall ensure the NSWC PHD computing plant is monitored and maintained in full compliance with the applicable directives listed in paragraph 2.0 of this SOW. Any deviations found shall result in generation of a resolution Plan of Action and Milestones (POAM) and be recorded per the Command Change Management process, and documented in monthly Contract Data Requirement List (CDRL) data deliverables.

The contractor shall create and submit orders and build-outs in network enabled technologies (NET).

The contractor shall validate rollovers and lookup records in NET.

The contractor shall perform eMarketplace (eMp) functions.

The contractor shall create Wide Area Workflow (WAWF) requests for CLIN 5000's CLIN 32'S 6ag's within the NMCI contract.

The contractor shall develop policies and plans that support/enhance their accomplishment within the organization's enterprise IT goals and objectives.

3.2.1.2 Application Maintenance

The contractor shall provide continuous support for maintenance, integration, configuration management, and documentation of corporate information systems, databases, commercial-off-the-shelf (COTS) systems, and client/server technologies for all in-service command applications.

The contractor shall maintain web applications, support web-based collaborative environments, maintain client facing services, and all helpdesk applications. Contractor shall modify/upgrade existing applications using Navy authorized tools.

3.2.2 IT Support

The contractor shall provide IT professionals who have an expert knowledge and experience to assist in the orderly operational support of corporate computing plants.

3.2.2.1 Help Desk

The contractor shall provide first level call support via existing telecom and/or IT infrastructure.

The contractor shall provide response/resolution of service calls. The contractor shall support queries to the Help Desk by the end user and ensure the expeditious closure of all open items.

The contractor shall perform continuous analysis of NSWC PHD’s Help Desk tracking tickets in order to define process and product trends, along with recommended courses of corrective action (CDRL A001).

3.2.2.2 IT Documentation Support

The contractor shall author, maintain, and provide updates to system documentation, quality assurance plans, and configuration management data to support various NSWC PHD IT systems.

The contractor shall support the Navy Enterprise IT system process and Federal Portfolio Management compliance processes of DoN Application and Database Management System, DoD Information Technology Portfolio Repository DoD/DoN Enterprise Architecture in accordance with paragraph 2.0 of this SOW.

The contractor shall ensure that the compliant documentation is produced to support command operations.

The contractor shall support documentation involved in Security Hardening of IT Hardware such as required DoD Cybersecurity RMF Assessment and Authorization Process.

The contractor shall review, update, and submit a report indicating total number of systems being supported and their accreditation status in writing weekly.

3.2.3 Portfolio Development

The contractor shall provide IT professionals who have an expert knowledge and experience in the development of integrated systems and software.

3.2.3.1 New Systems Development

The contractor shall provide software development and hardware integration services for implementation of IT solutions that support the stations mission, in accordance with the standards and guidance in paragraph 2.0 of this SOW.

The contractor shall provide support in the areas of design, development, integration, configuration management, and documentation for corporate information systems, databases, web-based applications, COTS and Government off the Shelf systems.

The contractor shall develop prototypes for Government approval. The contractor shall conduct testing of the prototype

to ensure that it meets all requirements identified prior to rollout.

3.2.3.2 Cloud Computing

The contractor shall provide continuous support for the Command's cloud computing environment that supports the NSWC PHD Command Corporate / RDT&E infrastructure.

The contractor shall support cloud-based server, platform and database infrastructure required to maintain operational availability and full compliance with Navy cybersecurity requirements. Server and application support is required 24 hours a day, seven days a week for the entire performance of this contract.

The contractor shall ensure that the NSWC PHD cloud computing environment is monitored and maintained in full compliance with paragraph 2.0 of this SOW. Any deviations found shall result in generation of a resolution POAM and be recorded per the Command Change Management process, and documented in monthly CDRLs.

3.2.4 Cybersecurity Support

Contractor shall provide Cybersecurity Workforce professionals who have expert knowledge and experience to assist in the information securing, monitoring, and documentation of corporate computing plants.

3.2.4.1 Cybersecurity Operations

The contractor shall provide Cybersecurity solutions that support NSWC PHD's mission in accordance with the standards and guidance in paragraph 2.0 of this SOW.

The contractor shall conduct hardening, testing and certification services for the NSWC PHD corporate computing plant (system/server/application/platform) and associated networks to ensure they meet all Navy Cybersecurity requirements.

3.2.4.2 Cybersecurity Documentation Support

The contractor shall author, maintain, and provide updates to system Accreditation and Authorization (A&A) documentation, quality assurance plans, configuration management data and security certification requirements to

support various NSWC PHD IT systems.

The contractor shall support the Navy RMF process and ensure successful A&A of IT systems required to execute the NSWC PHD Mission in accordance with paragraph 2.0 of this SOW.

The contractor shall ensure that all Command IT System A&A/RMF documentation is current and compliant with the cognizant Navy Approval Authority's continuous monitoring requirements (CDRLs A004 and A005).

The contractor shall support development, review, and updates of all required documentation involved in securing/accrediting/maintaining Command IT Systems/Platforms.

3.2.5 Technical Support Services

The contractor shall provide support for the existing NSWC PHD telephone system from the NSWC PHD demarcation point, Bldg. 1524 to the desktop phone unit. The contractor shall participate in the planning phase for new installations. The contractor shall maintain, program, and troubleshoot the entire voice communication network, consisting of CAT 3, 5, or 5e drops. The contractor shall maintain inventory, cable, fiber, manuals, and other relevant items, including work orders. The contractor shall manage the recurring monthly lease of telephone lines and associated equipment. The contractor shall provide support to NSWC PHD directory listing for directory assistance. The contractor shall support NSWC PHD for billing review, analysis, and ad-hoc reporting.

The contractor shall provide fiber and copper wiring services in support of moves, adds, changes, and large remodel projects. The contractor shall receive requests for services from the Help Desk support personnel. The incoming contractor is required to interface (via email) with the existing Help Desk contractor's personnel operators to acknowledge receipt of telephony service call records. The incoming contractor will then manage, from initiation to resolution, closure of the telephony service call records. These records will be compiled into a service request log. The service request log data shall be cumulative from contract issue date. The current month's service call activity shall be included in the monthly Contracting Officer's Management Report (CDRL A001).

The contractor shall provide support to maintain the current infrastructure. The contractor shall provide End User Training, to include training literature and hardware operating instructions. The contractor shall respond to the landline contract liaison personnel regarding any emergent issues or requirements.

Technical support services shall include the maintenance and service of the 6,709 phone lines envisioned, 200 Integrated Services Digital Network (ISDN) lines envisioned to support the multi-line capable units, the DISN support for the four ISDN Primary Rate Interface (PRI) lines supporting the Command VTC, and basic support of all fault isolation for phone circuits. Below is an itemized list of NSWC PHD's existing lines:

TYPE OF LINE	QUANTITY
Lobby	12
Elevator	5
Fire/Alarm	78
Fax	116
Analog	46
Polycom	55
PRI for VTC	4
VTC/Basic Rate Interface (BRI)	51
Secure Telephone Unit/Secure Telephone Equipment	80
BRI/Voice Multi Line Phone	145
9316/Single Line Phone	2,432
9417/Two Line Phone	36
Spare	31
TOTAL	**3,091**

The contractor shall provide engineering design recommendations as requested in anticipation of future growth of NSWC PHD personnel and associated telephony infrastructure.

The contractor shall provide coverage during high volume work projects. The contractor shall provide temporary support when the established workforce is out of the work place for more than a one-week period.

3.2.6 Materials

Materials to support hardware replacement and infrastructure, troubleshooting, test and repair, and maintenance of telephones is the responsibility of the contractor.

3.3 DATA DELIVERABLES

The contractor shall submit data deliverables as described in Exhibit A.

CLAUSES INCORPORATED BY FULL TEXT

C-202-H001 ADDITIONAL DEFINITIONS–BASIC (NAVSEA) (OCT 2018)

(a) Department - means the Department of the Navy.

(b) Commander, Naval Sea Systems Command - means the Commander of the Naval Sea Systems Command of the Department of the Navy or his duly appointed successor.

(c) References to The Federal Acquisition Regulation (FAR) - All references to the FAR in this contract shall be deemed to also reference the appropriate sections of the Defense FAR Supplement (DFARS), unless clearly indicated otherwise.

(d) National Stock Numbers - Whenever the term Federal Item Identification Number and its acronym FIIN or the term Federal Stock Number and its acronym FSN appear in the contract, order or their cited specifications and standards, the terms and acronyms shall be interpreted as National Item Identification Number (NIIN) and National Stock Number (NSN) respectively which shall be defined as follows:

(1) National Item Identification Number (NIIN). The number assigned to each approved Item Identification under the Federal Cataloging Program. It consists of nine numeric characters, the first two of which are the National Codification Bureau (NCB) Code. The remaining positions consist of a seven digit non-significant number.

(2) National Stock Number (NSN). The National Stock Number (NSN) for an item of supply consists of the applicable four-position Federal Supply Class (FSC) plus the applicable nine-position NIIN assigned to the item of supply.

(End of text)

C-204-H001 USE OF NAVY SUPPORT CONTRACTORS FOR OFFICIAL CONTRACT FILES (NAVSEA) (OCT 2018)

(a) NAVSEA may use a file room management support contractor, hereinafter referred to as "the support contractor", to manage its file room, in which all official contract files, including the official file supporting this procurement, are retained. These official files may contain information that is considered a trade secret, proprietary, business sensitive or otherwise protected pursuant to law or regulation, hereinafter referred to as “protected information”. File room management services consist of any of the following: secretarial or clerical support; data entry; document reproduction, scanning, imaging, or destruction; operation, management, or maintenance of paper-based or electronic mail rooms, file rooms, or libraries; and supervision in connection with functions listed herein.

(b) The cognizant Contracting Officer will ensure that any NAVSEA contract under which these file room management services are acquired will contain a requirement that:

(1) The support contractor not disclose any information;

(2) Individual employees are to be instructed by the support contractor regarding the sensitivity of the official contract files;

(3) The support contractor performing these services be barred from providing any other supplies and/or services, or competing to do so, to NAVSEA for the period of performance of its contract and for an additional three years thereafter unless otherwise provided by law or regulation; and,

(4) In addition to any other rights the contractor may have, it is a third party beneficiary who has the right of direct action against the support contractor, or any person to whom the support contractor has released or disclosed protected information, for the unauthorized duplication, release, or disclosure of such protected information.

(c) Execution of this contract by the contractor is considered consent to NAVSEA's permitting access to any information, irrespective of restrictive markings or the nature of the information submitted, by its file room management support contractor for the limited purpose of executing its file room support contract responsibilities.

(d) NAVSEA may, without further notice, enter into contracts with other contractors for these services. Contractors should enter into separate non-disclosure agreements with the file room contractor. Contact the Procuring Contracting Officer for contractor specifics. However, any such agreement will not be considered a prerequisite before information submitted is stored in the file room or otherwise encumber the government.

(End of text)

C-211-H017 UPDATING SPECIFICATIONS AND STANDARDS (NAVSEA) (DEC 2018)

The contractor may request that this contract be updated to include the current version of the applicable specification or standard if the update does not affect the form, fit or function of any deliverable item or increase the cost/price of the item to the Government. The contractor should submit update requests to the Procuring Contracting Officer with copies to the Administrative Contracting Officer and cognizant program office representative for approval. The contractor shall perform the contract in accordance with the existing specifications and standards until notified of approval/disapproval of its request to update by the Procuring Contracting Officer. Any approved alternate specifications or standards will be incorporated into the contract.

(End of text)

C-211-H018 APPROVAL BY THE GOVERNMENT (NAVSEA) (JAN 2019)

Approval by the Government as required under this contract and applicable specifications shall not relieve the Contractor of its obligation to comply with the specifications and with all other requirements of the contract, nor shall it impose upon the Government any liability it would not have had in the absence of such approval.

(End of text)

C-212-W002 COMMERCIAL SUPPLIER AGREEMENTS (NAVSEA) (MAR 2019)

(a) Commercial Supplier Agreement means End User License Agreement (EULA), Terms of Service (TOS), or similar legal instrument or agreement.

(b) Any Commercial Supplier Agreement must be provided in full text as part of a quote or offer without hyperlinks.

(c) The contract/order Schedule and Federal Acquisition Regulation (FAR) 52.212-4, Contract Terms and Conditions —Commercial Items, shall take precedence over any conflicting provisions in a Commercial Supplier Agreement.

(d) If any requirement in the Commercial Supplier Agreement conflicts with Federal law or regulations (see FAR 12.212(a)), the following shall apply:

(i) Any such requirement is unenforceable against the Government.

(ii) Neither the Government nor any Government authorized end user shall be deemed to have agreed to such requirement by virtue of it appearing in the Commercial Supplier Agreement. If the Commercial Supplier Agreement is invoked through an "I agree" click box or other comparable mechanism (e.g., "click-wrap" or "browse-wrap" agreements), execution does not bind the Government or any Government authorized end user to such requirement.

(iii) Any such requirement is deemed to be stricken from the Commercial Supplier Agreement

(e) Automatic renewals. License Agreements will expire at end of the term identified in the Purchase Order/Contract. Automatic renewals are not permitted and any such provision is void.

(f) Changes to the Commercial Supplier Agreement. Unilateral changes of the Commercial Supplier Agreement are impermissible and any requirement authorizing such changes is unenforceable. Changes must be in writing and executed by both parties to be effective.

(g) Third Part License (Embedded Software).

(i) The Contractor agrees that it has obtained all necessary licenses for the Government for any third party materials (including without limitation all Open Source licenses) provided within the product.

(ii) Contractor agrees that it complies with and shall continue to comply with all of its obligations under Third Party Licenses (including without limitation all Open Source licenses) associated with any third party materials provided within each product.

(iii) To the extent that the Government’s use of the software products licensed herein is in compliance with the Contractor’s Commercial Supplier Agreement, the Government’s use will also be in compliance with any Third Party Licenses.

(h) Audits. In lieu of any audit provisions in the Commercial Supplier Agreement, the Government agrees that, no more than once every twelve (12) months or within a reasonable time after a transfer, the Contractor shall, upon reasonable notice, have the right to require that the Government conduct an internal audit to ascertain and verify the number of licenses in use and to verify that the Government’s use of the product is in conformity with this Agreement. The Government is not required to use any tools provided by the Contractor to conduct the audit and shall not be required to pay for any tools provided by the Contractor to conduct the audit. The results of any such audit shall be kept confidential. If verification discloses that the Government’s use is not in conformity with this Agreement, the Government agrees to resolve any noncompliance by either removing or correcting the unlicensed installation and use of the software identified by the audit as not in conformity with this Agreement.

(i) Confidentiality. Commercial Supplier Agreements' terms and the final contract pricing may not be deemed confidential. Other marked confidential information will be appropriately guarded.

(j) Assignment. The Government shall have the right, without the prior written consent of the Contractor or its authorized resellers, to assign, reassign, or transfer software licenses among Government employees or the Government's rights in the Contractor's product to any governmental organization that is managed, operated, or controlled by the Government. Such authorization includes sublicensing, and assignment or transfer among or between authorized users. In the event authorized users are reorganized or restructured such that their responsibilities and operations are transferred to another government agency, the agency shall have the right to assign the affected program licenses to a successor agency. The licensed agency and the successor agency agree to be bound to the Commercial Supplier Agreement as modified. The transferee shall be bound by the license metrics and limitations in this license. Government shall complete any documentation required by the Contractor to facilitate the transfer of this license, and continuation of support shall be the responsibility of the transferee. For the avoidance of doubt, any assignment or transfer of licenses of the Contractor's products is also subject to all other terms of the Commercial Supplier Agreement, as well as the Contractor's policies governing product dependencies and version compatibility. Reassignment does not require that the license be under maintenance or support in order to execute a transfer.

(k) Litigation. Any requirement insisting that the commercial supplier or licensor control any litigation arising from the government's use of the contractor's supplies or services is deleted and unenforceable.

(l) Equitable Remedies. Equitable remedies, injunctive relief, and binding arbitration requirements shall not be enforced unless explicitly authorized by agency guidance or statute.

(m) Venue. Any claim or dispute shall be resolved under the Contract Disputes Act and FAR 52.233-1. The forum for resolution of disputes and applicable statutes of limitation shall be governed by federal law.

(n) Applicable law. In accordance with FAR 52.233-4, United States law shall apply to resolve any claim of breach of this contract and such actions shall be handled in the applicable Federal court of jurisdiction.

(End of text)

C-215-H002 CONTRACTOR PROPOSAL (NAVSEA) (OCT 2018)

(a) Performance of this contract by the Contractor shall be conducted and performed in accordance with the detailed obligations to which the Contractor committed itself in Proposal TBD dated TBD in response to Solicitation No. N6339419R3500.

(b) The technical volume(s) of the Contractor's proposal is(are) hereby incorporated by reference and made subject to the "Order of Precedence" (FAR 52.215-8) clause of this contract. Under the "Order of Precedence" clause, the technical volume(s) of the Contractor's proposal referenced herein is (are) hereby designated as item (f) of the clause, following "the specifications" in the order of precedence.

(End of text)

C-223-W002 ON-SITE SAFETY REQUIREMENTS (NAVSEA) (OCT 2018)

(a) The contractor shall ensure that each contractor employee reads any necessary safety documents within 30 days of commencing performance at any Government facility. Required safety documents can be obtained from the respective safety office. Contractors shall notify the Safety office points of contact below to report completion of the required training via email. The email shall include the contractor employee's name, work site, and contract number.

(b) It is expected that contractor employees will have received training from their employer on hazards associated with the areas in which they will be working and know what to do in order to protect themselves. Contractors are required to adhere to the requirements of 29 CFR 1910, 29 CFR 1926 and applicable state and local requirements while in Government spaces. The contractor shall ensure that all on-site contractor work at the Government facility is in accordance with any local safety instructions as provided via the COR. The contractor shall report all work-related injuries/illnesses that occurred while working at the Government site to the COR.

(c) Contractors whose employees perform work within Government spaces in excess of 1000 hours per calendar quarter during a calendar year shall submit the data elements on OSHA Form 300A, Summary of Work Related Injuries and Illnesses, for those employees to the safety office, via the COR by 15 January for the previous calendar year, even if no work related injuries or illnesses occurred. If a contractor's injury/illness rates are above the Bureau of Labor Statistics industry standards, a safety assessment may be performed by the Safety Office to determine if any administrative or engineering controls can be utilized to prevent further injuries/illnesses, or if any additional Personal Protective Equipment or training will be required.

(d) Any contractor employee exhibiting unsafe behavior may be removed from the Government site. Such removal shall not relieve the contractor from meeting its contractual obligations and shall not be considered an excusable delay as defined in FAR 52.249-14.

(e) The Safety Office points of contacts are as follows: Contact the COR for this information.

(End of text)

C-227-H006 DATA REQUIREMENTS (NAVSEA) (OCT 2018)

The data to be furnished hereunder shall be prepared in accordance with the Contract Data Requirements List, DD Form 1423, Exhibit(s) A, attached hereto.

(End of text)

C-227-H008 GOVERNMENT-INDUSTRY DATA EXCHANGE PROGRAM (NAVSEA) (DEC 2018)

(a) The contractor shall actively participate in the Government Industry Data Exchange Program in accordance with the GIDEP Operations Manual, S0300-BT-PRO-010. The contractor shall submit information concerning critical or major nonconformances, as defined in FAR 46.407/DFARS 246.407, to the GIDEP information system.

(b) The contractor shall insert paragraph (a) of this clause in any subcontract when deemed necessary. When so inserted, the word "contractor" shall be changed to "subcontractor."

(c) The contractor shall, when it elects not to insert paragraph (a) in a subcontract, provide the subcontractor any GIDEP data which may be pertinent to items of its manufacture and verify that the subcontractor utilizes any such data.

(d) The contractor shall, whether it elects to insert paragraph (a) in a subcontract or not, verify that the subcontractor utilizes and provides feedback on any GIDEP data that may be pertinent to items of its manufacture."

(e) GIDEP materials, software and information are available without charge from:

GIDEP Operations Center

P.O. Box 8000

Corona, CA 92878-8000

Phone: (951) 898-3207

FAX: (951) 898-3250

Internet: http://www.gidep.org

(End of text)

C-227-H009 ACCESS TO DATA OR COMPUTER SOFTWARE WITH RESTRICTIVE MARKINGS (NAVSEA) (JAN 2019)

(a) Performance under this contract may require that the Contractor have access to technical data, computer software, or other sensitive data of another party that contains restrictive markings. If access to such data or software is required or to be provided, the Contractor shall enter into a written agreement with such party prior to gaining access to such data or software. The agreement shall address, at a minimum, (1) access to, and use of, the restrictively marked data or software exclusively for the purposes of performance of the work required by this contract, and (2) safeguards to protect such data or software from unauthorized use or disclosure for so long as the data or software remains properly restrictively marked. In addition, the agreement shall not impose any limitation upon the Government or its employees with respect to such data or software. A copy of the executed agreement shall be provided to the Contracting Officer. The Government may unilaterally modify the contract to list those third parties with which the Contractor has agreement(s).

(b) The Contractor agrees to: (1) indoctrinate its personnel who will have access to the data or software as to the restrictions under which access is granted; (2) not disclose the data or software to another party or other Contractor personnel except as authorized by the Contracting Officer; (3) not engage in any other action, venture, or employment wherein this information will be used, other than under this contract, in any manner inconsistent with this requirement; (4) not disclose the data or software to any other party, including, but not limited to, joint venturer, affiliate, successor, or assign of the Contractor; and (5) reproduce the restrictive stamp, marking, or legend on each use of the data or software whether in whole or in part.

(c) These restrictions on use and disclosure of the data and software also apply to information received from the Government through any means to which the Contractor has access in the performance of this contract that contains restrictive markings.

(d) The Contractor agrees that it will promptly notify the Contracting Officer of any attempt to gain access to any information with restrictive markings. Such notification shall include the name and organization of the individual, company, or Government representative seeking access to such information.

(e) The Contractor shall include this requirement in subcontracts of any tier which involve access to information covered by paragraph (a), substituting "subcontractor" for "Contractor" where appropriate.

(f) Compliance with this requirement is a material requirement of this contract.

(End of text)

C-227-H010 COMPUTER SOFTWARE AND COMPUTER DATA BASES DELIVERED TO OR RECEIVED FROM THE GOVERNMENT (NAVSEA) (JAN 2019)

(a) The Contractor agrees to test for viruses, malware, Trojan Horses, and other security threats such as those listed in NIST Special Publication 800-12 Rev 1, An Introduction to Computer Security, The NIST Handbook, Chapter 4, in all computer software and computer data bases (as defined in the clause entitled "Rights In Noncommercial Computer Software and Noncommercial Computer Software Documentation" (DFARS 252.227-7014)), before delivery of that computer software or computer data base in whatever media and on whatever system the computer software or data base is delivered whether delivered separately or imbedded within delivered equipment. The Contractor warrants that when delivered any such computer software and computer data base shall be free of viruses, malware, Trojan Horses, and other security threats such as those listed in NIST Special Publication 800-12 Rev 1.

(b) The Contractor agrees that prior to use under this contract, it shall test any computer software and computer data base received from the Government for viruses, malware, Trojan Horses, and other security threats listed in NIST Special Publication 800-12 Rev 1, An Introduction to Computer Security, The NIST Handbook, Chapter 4.

(c) Any license agreement governing the use of any computer software or computer software documentation delivered to the Government as a result of this contract must be paid-up, irrevocable, world-wide, royalty-free, perpetual and flexible (user licenses transferable among Government employees and personnel under Government contract).

(d) The Contractor shall not include or permit to be included any routine to enable the contractor or its subcontractor(s) or vendor(s) to disable the computer software or computer data base after delivery to the Government.

(e) No copy protection devices or systems shall be used in any computer software or computer data base delivered under this contract with unlimited or Government purpose rights (as defined in DFARS 252.227-7013 and 252.227-7014) to restrict or limit the Government from making copies.

(f) It is agreed that, to the extent that any technical or other data is computer software by virtue of its delivery in digital form, the Government shall be licensed to use that digital-form data with exactly the same rights and limitations as if the data had been delivered as hard copy.

(g) Any limited rights legends or other allowed legends placed by a Contractor on technical data or other data delivered in digital form shall be digitally included on the same media as the digital-form data and must be associated with the corresponding digital-form technical data to which the legend(s) apply to the extent possible. Such legends shall also be placed in human-readable form on a visible surface of the media carrying the digital-form data as delivered, to the extent possible.

(End of text)

C-237-H001 ENTERPRISE-WIDE CONTRACTOR MANPOWER REPORTING APPLICATION (NAVSEA) (OCT 2018)

(a) The contractor shall report contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the Naval Surface Warfare Center Port Hueneme Division via a secure data collection site. Contracted services excluded from reporting are based on Product Service Codes (PSCs). The excluded PSCs are:

(1) W, Lease/Rental of Equipment;

(2) X, Lease/Rental of Facilities;

(3) Y, Construction of Structures and Facilities;

(4) D, Automatic Data Processing and Telecommunications, IT and Telecom- Telecommunications Transmission (D304) and Internet (D322) ONLY

(5) S, Utilities ONLY;

(6) V, Freight and Shipping ONLY.

(b) The contractor is required to completely fill in all required data fields using the following web address https://www.ecmra.mil.

(c) Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the help desk, linked at https://dod.ecmra.support.desk@mail.mil.

(End of text)

C-237-H002 SUBSTITUTION OF KEY PERSONNEL (NAVSEA) (OCT 2018)

(a) The Contractor agrees that a partial basis for award of this contract is the list of key personnel proposed. Accordingly, the Contractor agrees to assign to this contract those key persons whose resumes were submitted with the proposal necessary to fulfill the requirements of the contract. No substitution shall be made without prior notification to and concurrence of the Contracting Officer in accordance with this requirement. Substitution shall include, but not be limited to, subdividing hours of any key personnel and assigning or allocating those hours to another individual not approved as key personnel.

(b) All proposed substitutes shall have qualifications equal to or higher than the qualifications of the person to be replaced. The Contracting Officer shall be notified in writing of any proposed substitution at least forty five (45) days, or ninety (90) days if a security clearance is to be obtained, in advance of the proposed substitution. Such notification shall include: (1) an explanation of the circumstances necessitating the substitution; (2) a complete resume of the proposed substitute; (3) an explanation as to why the proposed substitute is considered to have equal or better qualifications than the person being replaced; (4) payroll record of the proposed replacement; and (5) any other information requested by the Contracting Officer to enable him/her to judge whether or not the Contractor is maintaining the same high quality of personnel that provided the partial basis for award.

(c) Key personnel are identified in an attachment in Section J.

(End of text)

C-237-W001 ELECTRONIC COST REPORTING AND FINANCIAL TRACKING (eCRAFT) SYSTEM REPORTING (NAVSEA) (MAY 2019)

(a) The Contractor agrees to upload the Contractor's Funds and Man-hour Expenditure Reports in the Electronic Cost Reporting and Financial Tracking (eCRAFT) System and submit the Contractor’s Performance Report on the day and for the same timeframe the contractor submits an invoice into the Wide Area Workflow (WAWF) module on the Procurement Integrated Enterprise Environment (PIEE) system. Compliance with this requirement is a material requirement of this contract. Failure to comply with this requirement may result in contract termination.

(b) The Contract Status Report indicates the progress of work and the status of the program and of all assigned tasks. It informs the Government of existing or potential problem areas.

(c) The Contractor’s Fund and Man-hour Expenditure Report reports contractor expenditures for labor, materials, travel, subcontractor usage, and other contract charges.

(1) Access: eCRAFT: Reports are uploaded through the eCRAFT System Periodic Report Utility (EPRU). The EPRU spreadsheet and user manual can be obtained at: http://www.navsea.navy.mil/Home/Warfare-Centers/NUWC-Newport/Partnerships/Commercial-Contracts/Information-eCraft-/under eCRAFT information. The link for eCRAFT report submission is: https://www.pdrep.csd.disa.mil/pdrep_files/other/ecraft.htm. If you have problems uploading reports, please see the Frequently Asked Questions at the site address above.

(2) Submission and Acceptance/Rejection: The contractor shall submit their reports on the same day and for the same timeframe the contractor submits an invoice in WAWF. The amounts shall be the same. eCRAFT acceptance/rejection will be indicated by e-mail notification from eCRAFT.

(End of text)

C-242-H001 EXPEDITING CONTRACT CLOSEOUT (NAVSEA) (OCT 2018)

(a) As part of the negotiated fixed price or total estimated amount of this contract, both the Government and the Contractor have agreed to waive any entitlement that otherwise might accrue to either party in any residual dollar amount of $1,000 or less at the time of final contract closeout. The term "residual dollar amount" shall include all money that would otherwise be owed to either party at the end of the contract, except that, amounts connected in any way with taxation, allegations of fraud and/or antitrust violations shall be excluded. For purposes of determining residual dollar amounts, offsets of money owed by one party against money that would otherwise be paid by that party may be considered to the extent permitted by law.

(b) This agreement to waive entitlement to residual dollar amounts has been considered by both parties. It is agreed that the administrative costs for either party associated with collecting such small dollar amounts could exceed the amount to be recovered.

(End of text)

C-242-H002 POST AWARD MEETNG (NAVSEA) (OCT 2018)

(a) A post-award meeting with the successful offeror will be conducted within 30 days after award of the task order. The meeting will be held at the address below:

Location/Address: Naval Surface Warfare Center Port Hueneme Division, 4363 Missile Way, Port Hueneme, CA 93043, or via teleconference.

(b) The contractor will be given 10 working days notice prior to the date of the meeting by the Contracting Officer.

(c) The requirement for a post-award meeting shall in no event constitute grounds for excusable delay by the contractor in performance of any provisions in the [contract / task order].

(d) The post-award meeting will include, but is not limited to, the establishment of work level points of contact, determining the administration strategy, roles and responsibilities, and ensure prompt payment and close out. Specific topics shall be mutually agreed to prior to the meeting.

(End of text)

C-242-H003 TECHNICAL INSTRUCTIONS (NAVSEA) (OCT 2018)

(a) Performance of the work hereunder may be subject to written technical instructions signed by the Contracting Officer and the Contracting Officer's Representative specified in Section G of this contract. As used herein, technical instructions are defined to include the following:

(1) Directions to the Contractor which suggest pursuit of certain lines of inquiry, shift work emphasis, fill in details or otherwise serve to accomplish the contractual statement of work.

(2) Guidelines to the Contractor which assist in the interpretation of drawings, specifications or technical portions of work description.

(b) Technical instructions must be within the general scope of work stated in the contract. Technical instructions may not be used to: (1) assign additional work under the contract; (2) direct a change as defined in the "CHANGES" clause of this contract; (3) increase or decrease the contract price or estimated contract amount (including fee), as applicable, the level of effort, or the time required for contract performance; or (4) change any of the terms, conditions or specifications of the contract.

(c) If, in the opinion of the Contractor, any technical instruction calls for effort outside the scope of the contract or is inconsistent with this requirement, the Contractor shall notify the Contracting Officer in writing within ten (10) working days after the receipt of any such instruction. The Contractor shall not proceed with the work affected by the technical instruction unless and until the Contractor is notified by the Contracting Officer that the technical instruction is within the scope of this contract.

(d) Nothing in the foregoing paragraph shall be construed to excuse the Contractor from performing that portion of the contractual work statement which is not affected by the disputed technical instruction.

(End of text)

C-246-H001 EXTENSION OF COMMERCIAL WARRANTY (NAVSEA) (OCT 2018)

The Contractor shall extend to the Government the full coverage of any standard commercial warranty normally offered in a similar commercial sale, provided that such warranty is available at no additional cost to the Government. The Contractor shall provide a copy of the standard commercial warranty with the item. The standard commercial warranty period shall begin upon the final acceptance of the applicable material or software. Acceptance of the standard commercial warranty does not waive the Government's rights under the "Inspection" clause, nor does it limit the Government's rights with regard to other terms and conditions of the contract. In the event of a conflict, the terms and conditions of the contract shall take precedence over the standard commercial warranty.

(End of text)